UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/687,075	10/16/2003	Bhawani Sapkota	72255/00004	8930

23380 7590 10/22/2007

TUCKER ELLIS & WEST LLP
1150 HUNTINGTON BUILDING
925 EUCLID AVENUE
CLEVELAND, OH 44115-1414

EXAMINER	
LE, CANH	

ART UNIT	PAPER NUMBER
2139	

NOTIFICATION DATE	DELIVERY MODE
10/22/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@tuckerellis.com
mary.erne@tuckerellis.com

Office Action Summary	Application No.	Applicant(s)	
	10/687,075	SAPKOTA ET AL.	
	Examiner	Art Unit	
	Canh Le	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 August 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16,18,19 and 22* is/are pending in the application.

4a) Of the above claim(s) *17,20,21 and 23-27* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16,18,19 and 22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/27/2005; 08/14/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to the application filed on 08/14/2007.

Claims 17, 20-21, and 23-27 have been cancelled.

Claims 1, 13, and 19 have been amended.

Claims 1-16, 18-19, and 22 have been examined and are pending.

Response to Arguments

Applicant's arguments filed 08/14/2007 have been fully considered but they are not persuasive.

With regard to claims 1 and 13, The Applicant argues that:

"The claims 1 and 13, as currently amended, are not anticipated by Cisco".

The Examiner respectfully disagrees:

Cisco teaches:

generating a client-specific management frame protection key [pg. 15, 4. Secure 802.11 Wireless LANs with Cisco Wireless Security Suite section; "All three of these components are included in the Cisco Wireless Security Suite:

.... Extensible Authentication Protocol (EAP) Cisco authentication algorithm -The EAP Cisco Wireless authentication type, also called Cisco LEAP supports centralized, user-based authentication with the ability to generate dynamic WEP keys"; a client-specific management frame protection key is equivalent to WEP keys; pg. 16-17; "Figure 24 802.1X and EAP message Flow ... This need has driven the

requirement for the authentication algorithm to generate keying material for dynamic WEP keys. Cisco LEAP employs its user-based nature to generate unique keying material for each client"].

deriving an information element based upon the client-specific management frame protection key for signing a management frame packet transmitted on the network [pg. 15, 4. Secure 802.11 Wireless LANs with Cisco Wireless Security Suite section; "All three of these components are included in the Cisco Wireless Security Suite... Extensible Authentication Protocol (EAP) Cisco authentication algorithm—The EAP Cisco Wireless authentication type, also called Cisco LEAP supports centralized, user-based authentication with the ability to generate dynamic WEP keys"; a client-specific management frame protection key is equivalent to WEP keys; pg. 16-17; "Figure 24 802.1X and EAP message Flow ... This need has driven the requirement for the authentication algorithm to generate keying material for dynamic WEP keys. Cisco LEAP employs its user-based nature to generate unique keying material for each client"];

With regard to claim 19, The Applicant argues that:

"The claim 19, as currently amended, are not anticipated by Cisco".

The Examiner respectfully disagrees:

Cisco teaches:

transmitting the management frame packet comprising the message integrity check value and the replay protection value to the access point [pg. 17, section 4.1.3.1

Message Integrity Check; a MIC adds two new field to a wireless frame: a sequence number and an integrity check field before transmitting; pg. 17-18, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; Modifications to any of the fields will result in a discrepancy in the calculated Message Integrity Check (MIC) on the receiver. As a result the receiver will drop the frame"] and

authenticating the message integrity check value and the replay protection value [pg. 15, section 4; a MIC function provides effective frame authenticity to mitigates man-in-the-middle vulnerabilities"; fig. 26; pg. 17-18, section 4.1.3.1 Message Integrity Check; "The sequence number is a sequential counter that increases in value on a per-frame, per-association basis. The access point will discard frames received that have an out-of-sequence number"].

Therefore, The Examine respectfully asserts that Cisco does teach the added limitations as provided by the amendment. The rejection for claims 1-16, 18-19, and 22 is maintained as given below, and the new limitations present in claims 1, 13, and 19 are addressed.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-16, 18-19, 22 are rejected under 35 U.S.C. 102(b) as being anticipated by **Cisco Systems**, "A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite", Pejman Roshan, August 2002, hereinafter Cisco.

As per claims 1, 13:

Cisco teaches a method/ a system for securing management frames, the method comprising the steps of:

(a) establishing an authenticated relationship between a transmitter and a receiver on a network **[pg. 2, section 2.2. 802.11 Station Authentication; fig. 1; authentication in the specification 802.11 is based on authenticating a wireless station or device instead of authenticating a user. Figure 1 shows authentication process between a wireless station and an access point]**;

(b) generating a client-specific management frame protection key **[pg. 15, 4. Secure 802.11 Wireless LANs with Cisco Wireless Security Suite section; "All three of these components are included in the Cisco Wireless Security Suite: .... Extensible Authentication Protocol (EAP) Cisco authentication algorithm—The EAP Cisco Wireless authentication type, also called Cisco LEAP supports centralized, user-based authentication with the ability to generate dynamic WEP keys"; a client-specific management frame protection key is equivalent to WEP keys; pg. 16-17; "Figure 24 802.1X and EAP message Flow ... This need has driven the requirement for the authentication algorithm to generate keying**

material for dynamic WEP keys. Cisco LEAP employs its user-based nature to generate unique keying material for each client"].

(c) deriving an information element based upon the client-specific management frame protection key for signing a management frame packet transmitted on the network **[pg. 15, 4. Secure 802.11 Wireless LANs with Cisco Wireless Security Suite section; "All three of these components are included in the Cisco Wireless Security Suite... Extensible Authentication Protocol (EAP) Cisco authentication algorithm—The EAP Cisco Wireless authentication type, also called Cisco LEAP supports centralized, user-based authentication with the ability to generate dynamic WEP keys"; a client-specific management frame protection key is equivalent to WEP keys; pg. 16-17; "Figure 24 802.1X and EAP message Flow ... This need has driven the requirement for the authentication algorithm to generate keying material for dynamic WEP keys. Cisco LEAP employs its user-based nature to generate unique keying material for each client"]**;

(d) embedding the information element into the management frame packet **[pg. 17, fig. 25, section 4.1.3.1. Message Integrity Check (MIC); fig. 26; MIC adds two new fields to a wireless frame: a sequence number and an integrity check field]**;

(e) transmitting the management frame packet to the receiver **[pg. 2; fig. 2; a probe request frame (i.e. management frame) is sent on every channel a client supports in an attempt to find all access points in range that match SSID and client-requested data rates]**;

(f) receiving the management frame packet **[pg. 2; "all access point that are in range and match the probe request criteria will respond with a probe response frame containing synchronization information and point load"]**; and

(g) validating the information element in the received management frame packet **[pg. 2; "all access point that are in range and match the probe request criteria will respond with a probe response frame containing synchronization information and point load"; matching the probe request criteria is equivalent to validating the information element].**

As per claims 2, 14:

Cisco teaches the method/ the system set forth in claim 1 wherein the information element includes a message integrity check information element **[pg. 17, fig. 25, section 4.1.3.1. Message Integrity Check (MIC); pg. 17-18, fig. 26; MIC adds two new fields to a wireless frame: a sequence number and an integrity check field];**

As per claim 3:

Cisco teaches the method set forth in claim 1 further comprising the steps of:

(a) generating a replay protection value for signing the management frame packet **[pg. 17-18, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; a sequence number (i.e. counter value) is a sequential counter that increases in value on a per-frame, per-association basis.**

Generating a replay protection value for signing the management frame is equivalent to increasing in value on the per-frame]; and

(b) adding the replay protection value into the management frame packet prior to transmitting **[pg. 17-18, fig. 26; a sequence number (SEQ) is added in WEP Frame format].**

As per claim 4:

Cisco teaches the method set forth in claim 3 further comprising the step of validating the replay protection value **[pg. 17, section 4.1.3. Data Privacy with TKIP and section 4.1.3.1. Message Integrity Check; "MIC adds a sequence number field to the wireless LAN. The access will drop frames received out of order"; "the MIC field provides a frame integrity check not vulnerable to the same mathematical shortcomings as an IVC"].**

As per claim 5:

Cisco teaches the method set forth in claim 1 wherein the step of generating a key is concurrent with the step of establishing an authenticated relationship **[pg. 16, figure 24; a derived key is concurrent in Client Authentication RADIUS server between client and RADIUS server].**

As per claim 6:

Cisco teaches the method set forth in claim 1 wherein the step of establishing an authenticated relationship further includes employing a key establishment protocol **[pg. 16, figure 24; a derived key is concurrent in Client Authentication RADIUS server between client and RADIUS server; pg. 33, item 4.; "The access point forward the EAP Identity Response to the AAA server using a RADIUS protocol message with Cisco vendor-specific attributes"].**

As per claim 7:

Cisco teaches the method set forth in claim 1 wherein the step of validating the information element further comprises the step of comparing the information element with a locally derived information element established by the receiver **[pg. 17-18, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; a sequence number (i.e. counter value) is a sequential counter that increases in value on a per-frame, per-association basis. An information element is included a sequence number; access point will discard frames (i.e. by comparing with its sequence number) received that have an out-of-order sequence number].**

As per claim 8:

Cisco teaches the method set forth in claim 2 wherein the step of validating the information element further comprises the step of comparing the message integrity check information element of the received management frame packet with a locally

derived message integrity check information element established by the receiver **[pg. 17-18, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; Modifications to any of the fields will result in a discrepancy in the calculated Message Integrity Check (MIC) on the receiver. As a result the receiver will drop the frame"].**

As per claim 9:

Cisco teaches the method set forth in claim 3 wherein the step of validating the information element further comprises the step of comparing the replay protection value of the received management frame packet with a locally derived replay protection value established by the receiver **[pg. 17-18, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; a sequence number (i.e. counter value) is a sequential counter that increases in value on a per-frame, per-association basis. Access point will discard frames (i.e. by comparing with its sequence number) received that have an out-of-order sequence number. A sequence number is equivalent a replay protection value].**

As per claim 10:

Cisco teaches the method set forth in claim 1 wherein the receiver includes an access point **[pg. 2, fig. 1; a client and access point authentication process].**

As per claim 11:

Cisco teaches the method set forth in claim 1 wherein the transmitter includes a wireless client **[pg. 2, fig. 1; a client and access point authentication process].**

As per claim 12:

Cisco teaches the method set forth in claim 2 further comprising the step of generating the message integrity check value for the management frame packet prior to transmitting **[pg. 17, fig. 25, section 4.1.3.1. Message Integrity Check (MIC); pg. 17-18, fig. 26; MIC adds two new fields to a wireless frame: a sequence number and an integrity check field; It is inherent that MIC generates ICV before adding into a wireless frame prior to transmitting].**

As per claim 15:

Cisco further teaches the system set forth in claim 14 wherein the information element further includes a replay protection value **[pg. 17-18, figure 26; a sequence number (SEQ) is included in WEP frame format].**

As per claim 16:

Cisco teaches the system set forth in claim 13 wherein the means for transmitting the management frame packet is an IEEE 802.11 protocol **[pg. 17-18, figure 26; 802.11 header is included in a WEP frame format].**

As per claim 18:

Cisco teaches the method set forth in claim 14, wherein the message integrity check information element uniquely identifies the management frame communication to the authenticator **[pg. 18, "The Cisco implementation of per-packet ... and processed normally (Figure 28); page 19, Per-packet keying ... packet keys will be generated"; per-packet keying will not generated the same packet key as unique IV/based WEP key pairs are used].**

As per claim 19:

Cisco teaches a method for preventing IEEE 802.11 session disruption on a network, comprising the steps of:

(a) establishing a communication link between an access point and a wireless client on the network **[pg. 2, section 2.2 802.11 Station Authentication; client and access point authentication process].**

(b) creating a trust relationship between the access point and the wireless client such that the wireless client is adapted to securely access the network **[pg. 2, section 2.2 802.11 Station Authentication; client and access point authentication process]**;

(c) establishing a client-specific key for signing a management frame packet configured to be transmitted between the access point and the wireless client **[pg. 15, section 4. Secure 802.11 Wireless LANs with Cisco Wireless Security Suite; "per-packet keying provides every frame with a new and unique WEP key that mitigates WEP key derivation attacks"]**

(d) generating a message integrity check value based upon the client-specific key **[pg. 17, section 4.1.3. Data Privacy with TKIP; TKIP provides two majors enhancements to WEP: MIC and per-packet keying for all WEP-encrypted data frames];**

(e) calculating a replay protection value for signing the management frame packet **[pg. 18, "a sequence number is a sequential counter that increases in value on a per-frame, per-association basis"].**

(f) embedding the message integrity check value and the replay protection value into the management frame packet **[pg. 17, section 4.1.3.1 Message Integrity Check; a MIC adds two new field to a wireless frame: a sequence number and an integrity check field before transmitting]**;

(g) transmitting the management frame packet comprising the message integrity check value and the replay protection value to the access point **[pg. 17, section 4.1.3.1 Message Integrity Check; a MIC adds two new field to a wireless frame: a sequence number and an integrity check field before transmitting; pg. 17-18, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; Modifications to any of the fields will result in a discrepancy in the calculated Message Integrity Check (MIC) on the receiver. As a result the receiver will drop the frame"]** and

(h) authenticating the message integrity check value and the replay protection value **[pg. 15, section 4; a MIC function provides effective frame authenticity to mitigates man-in-the-middle vulnerabilities"; fig. 26; pg. 17-18, section 4.1.3.1**

Message Integrity Check; "The sequence number is a sequential counter that increases in value on a per-frame, per-association basis. The access point will discard frames received that have an out-of-sequence number"].

As per claim 22:

Cisco teaches the method set forth in claim 19 wherein the step of authenticating further comprises the steps of:

(a) calculating a local replay protection value **[pg. 17-18, fig. 26; "a sequence number is a sequential counter that increases in value on a per-frame, per-association basis"].**

(b) generating a local message integrity check value **[pg. 17-18, fig. 27 MIC value derivation. "Modification to any of the fields will result in discrepancy in the calculated MIC on the receiver"];**

(c) comparing the received replay protection value with the local replay protection value **[pg. 17-18, "Figure 26 Example of WEP Frame ... the MIC requires the use of Cisco clients and access points"; a sequence number (i.e. counter value) is a sequential counter that increases in value on a per-frame, per-association basis. Access point will discard frames (i.e. by comparing with its sequence number) received that have an out-of-order sequence number. A sequence number is equivalent a replay protection value]**; and

(d) comparing the received message integrity check value with the local message integrity check value **[pg. 17-18, "Figure 26 Example of WEP Frame ... the MIC**

requires the use of Cisco clients and access points"; Modifications to any of the fields will result in a discrepancy in the calculated Message Integrity Check (MIC) on the receiver. As a result the receiver will drop the frame"].

Action is Final

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure.

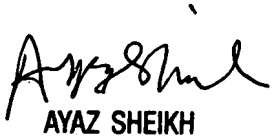
US 2004/0243846 A1 to Aboba et al.;

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Canh Le
October 13, 2007



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100